The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Acresso -- FLEXnet Connect	Acresso InstallShield Update Agent does not properly verify the authenticity of Rule Scripts obtained from GetRules.asp web pages on FLEXnet Connect servers, which allows remote man-in-the-middle attackers to execute arbitrary VBScript code via Trojan horse Rules.	2008-09-18	9.3	CVE-2008-1093 CERT-VN MISC BID BUGTRAQ
adobe -- illustrator	Multiple unspecified vulnerabilities in Adobe Illustrator CS2 on Macintosh allow user-assisted attackers to execute arbitrary code via a crafted AI file.	2008-09-18	9.3	CVE-2008-3961 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in Apple Type Services (ATS) in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allows remote attackers to execute arbitrary code via a document containing a crafted font, related to "PostScript font names."	2008-09-16	9.3	CVE-2008-2305 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	ImageIO in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allows context-dependent attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via a crafted TIFF image.	2008-09-16	9.3	CVE-2008-2332 BID
apple -- mac_os_x apple -- mac_os_x_server	ImageIO in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allows context-dependent attackers to cause a denial of service (memory corruption and	2008-09-16	9.3	CVE-2008-3608 BID

	application crash) or execute arbitrary code via a crafted JPEG image with an embedded ICC profile.			
apple -- mac_os_x apple -- mac_os_x_server	The kernel in Apple Mac OS X 10.5 through 10.5.4 does not properly flush cached credentials during recycling (aka purging) of a vnode, which might allow local users to bypass the intended read or write permissions of a file.	2008-09-16	7.2	CVE-2008-3609 BID
apple -- mac_os_x apple -- mac_os_x_server	Race condition in Login Window in Apple Mac OS X 10.5 through 10.5.4, when a blank-password account is enabled, allows attackers to bypass password authentication and login to any account via multiple attempts to login to the blank-password account, followed by selection of an arbitrary account from the user list.	2008-09-16	7.6	CVE-2008-3610 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Multiple integer overflows in the SearchKit API in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allow context-dependent attackers to cause a denial of service (application crash) or execute arbitrary code via vectors associated with "passing untrusted input" to unspecified API functions.	2008-09-16	10.0	CVE-2008-3616 BID APPLE
apple -- mac_os_x	The File Sharing pane in the Sharing preference pane in Apple Mac OS X 10.5 through 10.5.4 does not inform users that the complete contents of their own home directories are shared for their own use, which might allow attackers to leverage other vulnerabilities and access files for which sharing was unintended.	2008-09-16	9.0	CVE-2008-3618 CERT-VN BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	VideoConference in Apple Mac OS X 10.4.11 and 10.5 through 10.5.4 allows remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via vectors involving H.264 encoded media.	2008-09-16	9.3	CVE-2008-3621 BID
apple -- itunes apple -- quicktime	Heap-based buffer overflow in Apple QuickTime 7.5.5 and iTunes 8.0 allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a long type attribute in a quicktime tag (1) on a web page or embedded in a (2) .mp4 or (3) .mov file.	2008-09-18	9.3	CVE-2008-4116 BID MILW0RM
cisco -- ios	Multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 on the 871 Integrated Services Router allow remote attackers to execute arbitrary commands via (1) a certain "show privilege" command to the /level/15/exec/- URI, and (2) a certain	2008-09-18	9.3	CVE-2008-4128 BID MILW0RM MILW0RM

	"alias exec" command to the /level/15/exec/-/configure/http URI. NOTE: some of these details are obtained from third party information.			
flip4mac -- flip4mac_wmv	Multiple unspecified vulnerabilities in Flip4Mac WMV before 2.2.1 have unknown impact and attack vectors, different vulnerabilities than CVE-2007-6713.	2008-09-16	10.0	CVE-2008-4095 CONFIRM
ibm -- websphere_application_server	Unspecified vulnerability in Servlet Engine/Web Container in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.19, when the FileServing feature is enabled, has unknown impact and attack vectors.	2008-09-16	9.3	CVE-2008-4111 FRSIRT AIXAPAR SECUNIA
joomla -- joomla	Joomla! 1.5 before 1.5.7 initializes PHP's PRNG with a weak seed, which makes it easier for attackers to guess the pseudo-random values produced by PHP's mt_rand function, as demonstrated by guessing password reset tokens, a different vulnerability than CVE-2008-3681.	2008-09-18	7.5	CVE-2008-4102 MISC MISC BUGTRAQ MLIST MLIST MLIST CONFIRM
joomla -- joomla	JRequest in Joomla! 1.5 before 1.5.7 does not sanitize variables that were set with JRequest::setVar, which allows remote attackers to conduct "variable injection" attacks and have unspecified other impact.	2008-09-18	7.5	CVE-2008-4105 SECTRACK MLIST MLIST MLIST CONFIRM
landesk -- landesk_management_suite landesk -- landesk_security_suite landesk -- landesk_server_manager	Multiple buffer overflows in the QIP Server Service (aka qipsrvr.exe) in LANDesk Management Suite, Security Suite, and Server Manager 8.8 and earlier allow remote attackers to execute arbitrary code via a crafted heal request, related to the StringToMap and StringSize arguments.	2008-09-18	10.0	CVE-2008-2468 BID CONFIRM
macrovision -- flexnet_connect	The InstallShield Update Service Agent ActiveX control in isusweb.dll allows remote attackers to cause a denial of service (memory corruption and browser crash) and possibly execute arbitrary code via a call to ExecuteRemote with a URL that results in a 404 error response.	2008-09-18	9.3	CVE-2008-2470 CERT-VN
microsoft -- sql_server	Buffer overflow in the SQLVDIRLib.SQLVDirControl ActiveX control in Tools\Binn\sqlvdir.dll in Microsoft SQL Server 2000 (aka SQL Server 8.0) allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a long URL in the second argument to the Connect method. NOTE: this issue might only be exploitable in limited browser configurations.	2008-09-16	10.0	CVE-2008-4110 BID BUGTRAQ

microsoft -- windows-nt	srv.sys in Microsoft Windows Vista SP1 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a SMB WRITE_ANDX packet with an offset that is inconsistent with the packet size, as demonstrated by a request to the \PIPE\lsarpc named pipe.	2008-09-16	7.1	CVE-2008-4114 MISC BID MISC
phpmyadmin -- phpmyadmin	libraries/database_interface.lib.php in phpMyAdmin before 2.11.9.1 allows remote authenticated users to execute arbitrary code via a request to server_databases.php with a sort_by parameter containing PHP sequences, which are processed by create_function.	2008-09-18	8.5	CVE-2008-4096 MLIST
python_software_foundation -- python	Tools/faqwiz/move-faqwiz.sh (aka the generic FAQ wizard moving tool) in Python 2.4.5 might allow local users to overwrite arbitrary files via a symlink attack on a tmp$RANDOM.tmp temporary file. NOTE: there may not be common usage scenarios in which tmp$RANDOM.tmp is located in an untrusted directory.	2008-09-18	7.2	CVE-2008-4108 CONFIRM XF BID MLIST MLIST CONFIRM
sun -- management_center	Unspecified vulnerability in a web page in the PRM module in Sun Management Center (SunMC) 3.6.1 and 4.0 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	2008-09-18	7.8	CVE-2008-4117 SUNALERT
trend_micro -- client-server-messaging_security trend_micro -- officescan	Stack-based buffer overflow in cgiRecvFile.exe in Trend Micro OfficeScan 7.3 patch 4 build 1362 and other builds, OfficeScan 8.0 and 8.0 SP1, and Client Server Messaging Security 3.6 allows remote attackers to execute arbitrary code via an HTTP request containing a long ComputerName parameter.	2008-09-16	10.0	CVE-2008-2437 BID
vim -- vim	Vim 3.0 through 7.x before 7.2.010 does not properly escape characters, which allows user-assisted attackers to (1) execute arbitrary shell commands by entering a K keystroke on a line that contains a ";" (semicolon) followed by a command, or execute arbitrary Ex commands by entering an argument after a (2) "Ctrl-]" (control close-square-bracket) or (3) "g]" (g close-square-bracket) keystroke sequence, a different issue than CVE-2008-2712.	2008-09-18	9.3	CVE-2008-4101 MLIST MISC

Back to top

Medium Vulnerabilities

Primary	Description	Discovered	CVSS	Source & Patch

Vendor -- Product		Published	Score	Info
joomla -- com_mailto	The mailto (aka com_mailto) component in Joomla! 1.5 before 1.5.7 sends e-mail messages without validating the URL, which allows remote attackers to transmit spam.	2008-09-18	5.0	CVE-2008-4103 MLIST MLIST MLIST CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Network Preferences in Apple Mac OS X 10.4.11 stores PPP passwords in cleartext in a world-readable file, which allows local users to obtain sensitive information by reading this file.	2008-09-16	4.9	CVE-2008-2312 BID APPLE
apple -- mac_os_x_server	slapconfig in Directory Services in Apple Mac OS X 10.5 through 10.5.4 allows local users to select a readable output file into which the server password will be written by an OpenLDAP system administrator, related to the mkfifo function, aka an "insecure file operation issue."	2008-09-16	4.9	CVE-2008-2330 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Finder in Apple Mac OS X 10.5 through 10.5.4 does not properly update permission data in the Get Info window after a lock operation that modifies Sharing & Permissions in a filesystem, which might allow local users to leverage weak permissions that were not intended by an administrator.	2008-09-16	5.0	CVE-2008-2331 BID
apple -- mac_os_x apple -- mac_os_x_server	Login Window in Apple Mac OS X 10.4.11 does not clear the current password when a password-change attempt is denied by policy, which allows opportunistic, physically proximate attackers to bypass authentication and change this user's password by later entering an acceptable new password on the same login screen.	2008-09-16	6.3	CVE-2008-3611 BID
apple -- mac_os_x	Finder in Apple Mac OS X 10.5.2 through 10.5.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors involving a search for a remote disk on the local network.	2008-09-16	6.1	CVE-2008-3613 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Remote Management and Screen Sharing in Apple Mac OS X 10.5 through 10.5.4, when used to set a password for a VNC viewer, displays additional input characters beyond the maximum password length, which might make it easier for attackers to guess passwords that the user believed were longer.	2008-09-16	5.0	CVE-2008-3617 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Cross-site scripting (XSS) vulnerability in Wiki Server in Apple Mac OS X 10.5 through 10.5.4 allows remote attackers to inject arbitrary web script or HTML via an e-mail message that reaches a mailing-list archive, aka "persistent JavaScript injection."	2008-09-16	4.3	CVE-2008-3622 BID APPLE
apple -- iphone apple -- ipod_touch	Off-by-one error in the _web_drawInRect:withFont:ellipsis:alignment:measureOnly function in WebKit in Safari in Apple iPhone 1.1.4 and 2.0 and iPod touch 1.1.4 and 2.0 allows remote attackers to cause a denial of service (browser crash) via a JavaScript alert call with an argument that lacks breakable characters and has a length that is a multiple of the memory page size, leading to an out-of-bounds read.	2008-09-16	5.0	CVE-2008-3950 BID MISC

debian -- python-dns	PyDNS (aka python-dns) before 2.3.1-4 in Debian GNU/Linux does not use random source ports or transaction IDs for DNS requests, which makes it easier for remote attackers to spoof DNS responses, a different vulnerability than CVE-2008-1447.	2008-09-18	6.4	CVE-2008-4099 MLIST MLIST CONFIRM CONFIRM
debian -- python-dns	PyDNS (aka python-dns) before 2.3.1-5 in Debian GNU/Linux does not use random source ports for DNS requests and does not use random transaction IDs for DNS retries, which makes it easier for remote attackers to spoof DNS responses, a different vulnerability than CVE-2008-1447. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4099.	2008-09-18	6.4	CVE-2008-4126 MLIST MLIST CONFIRM CONFIRM
gallery -- gallery	Gallery before 1.5.9, and 2.x before 2.2.6, does not set the secure flag for the session cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.	2008-09-18	5.0	CVE-2008-3662 CONFIRM CONFIRM
gallery -- gallery	Gallery before 1.5.9, and 2.x before 2.2.6, does not properly handle ZIP archives containing symbolic links, which allows remote authenticated users to conduct directory traversal attacks and read arbitrary files via vectors related to the archive upload (aka zip upload) functionality.	2008-09-18	4.0	CVE-2008-4129 BID CONFIRM CONFIRM
gallery -- gallery	Cross-site scripting (XSS) vulnerability in Gallery 2.x before 2.2.6 allows remote attackers to inject arbitrary web script or HTML via a crafted Flash animation, related to the ability of the animation to "interact with the embedding page."	2008-09-18	4.3	CVE-2008-4130 CONFIRM
gnu -- adns	GNU adns 1.4 and earlier uses a fixed source port and sequential transaction IDs for DNS requests, which makes it easier for remote attackers to spoof DNS responses, a different vulnerability than CVE-2008-1447. NOTE: the vendor reports that this is intended behavior and is compatible with the product's intended role in a trusted environment.	2008-09-18	6.4	CVE-2008-4100 MLIST MLIST MILW0RM CONFIRM
high_norm -- sound_master_2nd	Cross-site scripting (XSS) vulnerability in High Norm Sound Master 2nd 1.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-09-18	4.3	CVE-2008-4118 IPA-JPCERT
joomla -- joomla	Multiple open redirect vulnerabilities in Joomla! 1.5 before 1.5.7 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a "passed in" URL.	2008-09-18	5.8	CVE-2008-4104 MLIST MLIST MLIST CONFIRM
linux -- kernel	The sctp_getsockopt_hmac_ident function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, relies on an untrusted length value to limit copying of data from kernel memory, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function.	2008-09-16	4.7	CVE-2008-4113 MISC BUGTRAQ CONFIRM CONFIRM

microsoft -- ie	Mshtml.dll in Microsoft Internet Explorer 7 Gold 7.0.5730 and 8 Beta 8.0.6001 on Windows XP SP2 allows remote attackers to cause a denial of service (failure of subsequent image rendering) via a crafted PNG file, related to an infinite loop in the CDwnTaskExec::ThreadExec function.	2008-09-18	4.3	CVE-2008-4127 BID BUGTRAQ
mysql -- mysql	MySQL 5.0.51a allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are associated with symlinks within pathnames for subdirectories of the MySQL home data directory, which are followed when tables are created in the future. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-2079.	2008-09-18	4.6	CVE-2008-4097 MLIST MLIST CONFIRM
mysql -- mysql	MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.	2008-09-18	4.6	CVE-2008-4098 CONFIRM
openbsd -- openssh	A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch, and before 4.6p1-1 on sid and lenny, uses functions that are not async-signal-safe in the signal handler for login timeouts, which allows remote attackers to cause a denial of service (connection slot exhaustion) via multiple login attempts. NOTE: this issue exists because of an incorrect fix for CVE-2006-5051.	2008-09-18	5.0	CVE-2008-4109 DEBIAN
php -- php	The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.	2008-09-18	5.1	CVE-2008-4107 FEDORA FEDORA MISC MISC MISC MISC BUGTRAQ BUGTRAQ MLIST FRSIRT CONFIRM SECTRACK SECUNIA SECUNIA MLIST
phpbb -- phpbb	The search function in phpBB 2.x provides a search_id value that leaks the state of PHP's PRNG, which allows remote attackers to obtain potentially sensitive information, as demonstrated by a cross-application attack against WordPress, a different vulnerability than CVE-2006-0632.	2008-09-18	5.0	CVE-2008-4125 MISC
talkback -- talkback	TalkBack 2.3.6 allows remote attackers to obtain configuration information via a direct request to	2008-09-16	5.0	CVE-2008-4115 MILW0RM

	install/info.php, which calls the phpinfo function.			
twiki -- twiki	Directory traversal vulnerability in bin/configure in TWiki before 4.2.3, when a certain step in the installation guide is skipped, allows remote attackers to read arbitrary files via a query string containing a .. (dot dot) in the image variable, and execute arbitrary files via unspecified vectors.	2008-09-18	6.8	CVE-2008-3195 CERT-VN
twiki -- twiki	Directory traversal vulnerability in bin/configure in TWiki before 4.2.3, when a certain step in the installation guide is skipped, allows remote attackers to read arbitrary files via a query string containing a .. (dot dot) in the image variable.	2008-09-16	5.0	CVE-2008-4112 CERT-VN
wordpress -- wordpress	WordPress before 2.6.2 does not properly handle MySQL warnings about insertion of username strings that exceed the maximum column width of the user_login column, and does not properly handle space characters when comparing usernames, which allows remote attackers to change an arbitrary user's password to a random value by registering a similar username and then requesting a password reset, related to a "SQL column truncation vulnerability." NOTE: the attacker can discover the random password by also exploiting CVE-2008-4107.	2008-09-18	5.1	CVE-2008-4106 CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
apple -- mac_os_x apple -- mac_os_x_server	Directory Services in Apple Mac OS X 10.5 through 10.5.4, when Active Directory is used allows attackers to enumerate user names via wildcard characters in the Login Window.	2008-09-16	1.9	CVE-2008-2329 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Time Machine in Apple Mac OS X 10.5 through 10.5.4 uses weak permissions for Time Machine Backup log files, which allows local users to obtain sensitive information by reading these files.	2008-09-16	2.1	CVE-2008-3619 BID APPLE
postfix -- postfix	Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.	2008-09-12	2.1	CVE-2008-3889 CONFIRM

Back to top